EA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

27510 7590 06/27/2005

KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER	
JARRETT, SCOTT L	
ART UNIT	**PAPER NUMBER**
3623	

DATE MAILED: 06/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

EA

Office Action Summary	Application No.	Applicant(s)
	09/805,279	BARNHART, ROBERT M.
	Examiner	Art Unit
	Scott L. Jarrett	3623

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This Final Office Action is responsive to Applicants remarks and amendment filed March 3, 2005. Applicants amendment amended claims 1-14, 19-22 and 27; currently claims 1-28 are pending.

Response to Amendment

2. The objection to Claims 5, 13, 19, 24 and 27 in the First Office Action is **withdrawn** in response to the Applicants amendment to Claims 5, 13, 19, 24 and 27.

Response to Arguments

3. Applicants arguments with regards to the 35 U.S.C. ℈ 101 rejection of Claims 1-14 have been fully considered and are deemed persuasive. The 35 U.S.C. ℈ 101 rejection of Claims 1-14 has been withdrawn.

4. Applicants arguments filed March 3, 2005 have been fully considered but they are not persuasive. In the Applicants remarks the Applicant argued:

- regarding the 35 U.S.C. ℈ 103(a) rejections of Claims 1-28 (see Pages 12-21):
    - applicant argues that the art of record does not teach:
        - that the ballot choices (vote) is digitally signed using the individual's private key as the claim now reads (Page 12);
        - recording in the data store the servers digital signature of the ballot for allowing verification at the server that all of the ballots that have been cast have not been tampered with or the specific verification by reconstruction steps as claimed (Pages 14-15);
        - storing an individual's (voter's) private encryption key, a certificate for the individual's public key (Page 15);
        - the generation of a voter identification when the voters registers to vote (Page 15);
        - creating an election voter table (Page 16);
        - comparing each ballot to the encrypted individual's voter identification to detect in an individual attempts to cast more than one ballot (duplicate ballot; Page 16);

- applicant argues that in Sehr's the definition of "demographics" is inconsistent with the that use of demographics as recited in the specification (Page 19); and
- applicant requests support for the following officially noticed facts:
  - the signing of a voting record and sending the signed voting record to the voter for allowing voter to keep a copy of his/her vote (Page 12-13);
  - the representation of documents (ballots) as images and that the corruption/defrauding of an image is more difficult that corrupting plain text (Page 17); and
  - the utilization of one-way hash functions for data integrity (Page 18).

5. The Applicants arguments with respect to the 35 U.S.C. ∍ 103(a) rejection of Claims 1-28 have been fully considered and are not persuasive. The 35 U.S.C. ∍ 103(a) rejections of Claims 1-28 are **not** withdrawn.

6. As per applicants arguments that the art of record does not teach that the ballot choices (vote) are digitally signed using the individual's private key (Page 12, Claims 1 and 15) Karro et al. teach a method and system for securely voting over a network (Abstract) wherein the system utilizes the well known and well established public key encryption scheme wherein voters are assigned a public/private pair key ("Eligible voters generate public/**private** key pairs for **signing** ballots...", Page 3, Paragraph 1;

Registration Phase: Step 3 "the authenticator generates a unique pair of public/private keys for the ID it received (i.e. the voter's ID) and stores them....", Page 4; Registration Phase Step 4: "The registrar then send the pair (private/public key) to the voter....").

Menezes et al. (Handbook of Applied Cryptography), as cited in the First Office Action, teach that the well known and established practice of cryptography is "...about the prevention and detection of cheating and other malicious activities. This book describes a number of basic cryptographic tools (**primitives**) used to provide information security. Examples of primitives include encryption schemes (x1.5 and x1.8), hash functions (x1.9), and digital signature schemes (x1.6). Figure 1.1 provides a schematic listing of the primitives considered and how they relate. " (Menezes et al.: Page 4; Page 5, Paragraph 1).

Menezes et al. further teach that "The encryption method is said to be a public-key encryption scheme if for each associated encryption/decryption pair (e; d), one key e (the public key) is made publicly available, while the other d (the private key) is kept secret" (Page 27, Paragraph 1; Figure 3 as shown below). Menezes et al. further clarifies public key encryption "To avoid ambiguity, a common convention is to use the term private key in association with public-key cryptosystems, and secret key in association with symmetric-key cryptosystems. This may be motivated by the following line of thought: it takes two or more parties to share a secret, but a key is truly private only when one party alone knows it." (Menezes et al: Page 27, Paragraph 2).

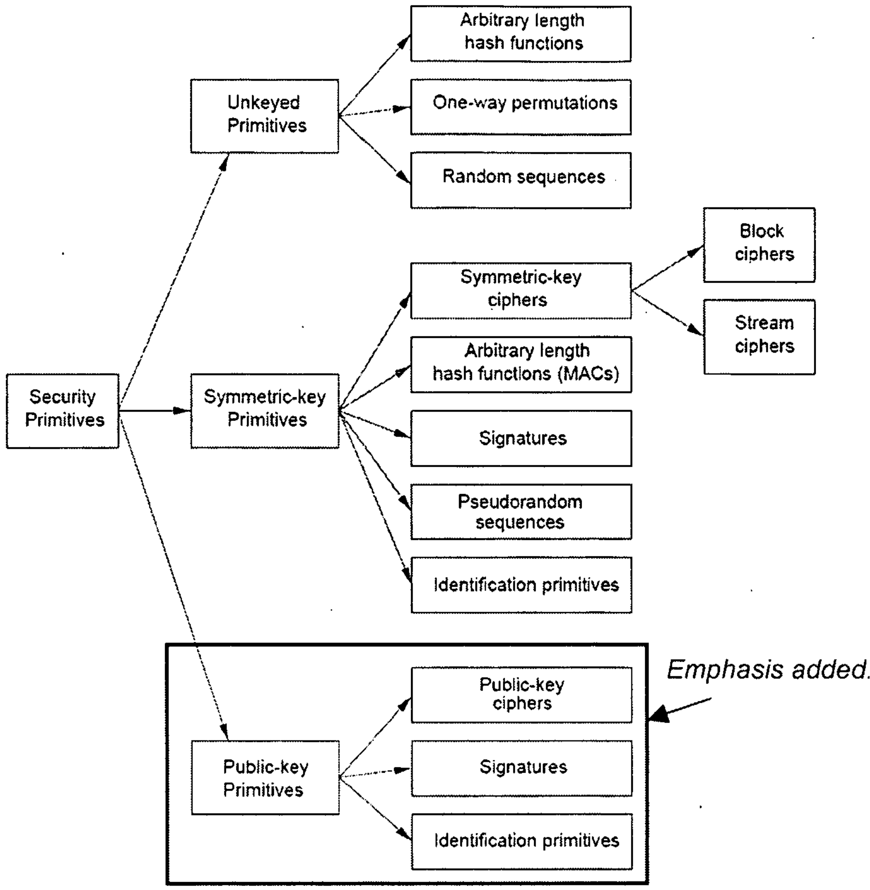

Figure 1.1: A taxonomy of cryptographic primitives.

Figure 1: Menezes et al.; Handbook of Applied Cryptography: Page 5

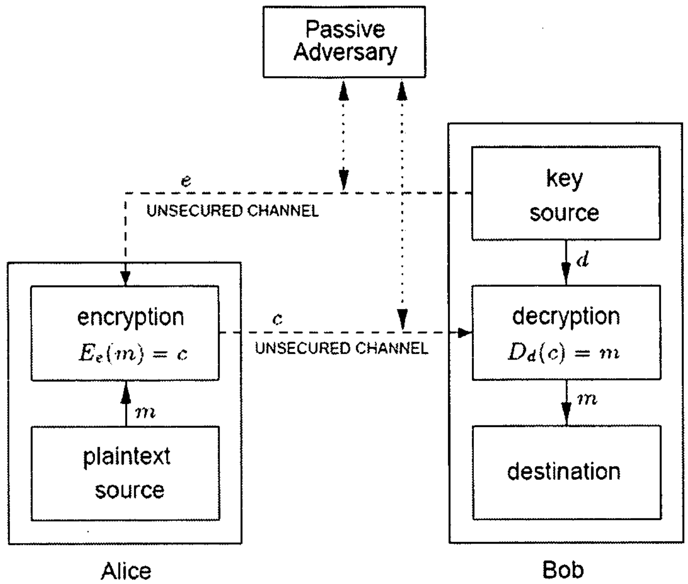

Figure 1.11: Encryption using public-key techniques.

Figure 2: Menezes et al.; Handbook of Applied Cryptography: Page 26

7. As per applicants arguments that the claims require confirming the retention of the vote at the server by signing a specific set of data elements (i.e. a confirmation) and transmitting of the signed confirmation to the voter (individual who submitted the ballot; Pages 12-13) Karro et al. teach that the method and system for securely voting over a network further comprises transmitting (sending) of a signed vote confirmation (receipt) by the system to the voter ("the tallier (i.e. system, server) signs the encrypted ballot x and returns it to the voters as a **receipt**...", Page 3, Paragraph 8; Voting Phase: Step 9 "...voter's browser generates a **receipt** when the authenticator confirms receiving the ballot..", Page 5; Lemma 3 "Due to the fact that voters are given a **receipt**, and that they are allowed to view the published lists as described in the Announcement Phase, a voter's vote cannot be altered, duplicated, or removed without being detected.", Page 7).

8. As per applicants arguments that the art of record does not disclose recording/storing in a data store the server's digital signature of the ballot (i.e. the server digitally signing the ballot to establish the receipt of the ballot by the server/system; Pages 14-15, Claims 3, 4, 17 and 18) Karro et al. teaches that the method and system for securely voting over a network records/stores in several data stores (databases) and subsystems the plurality of information (voter signed ballots, etc.) each subsystem receives ("Each facility is required to encrypt its database (list of data) on the fly, e.g. one record at a time, using the public keys of all the facilities....the database is encrypted piece by piece, the facility can easily extract the portion of data from the database it needs and send it to the other facilities to decrypt it.", Page 6 Paragraph 2) and that the encryption "...would also make it very easy to see any discrepancy in the results....", Page 6, Paragraph 3).

Karro et al. further teach that the method and system for securely voting over a network enables the public to verify the results utilizing a plurality of means including but not limited to the verification of the election by the verifier subsystem wherein the subsystem compares the lists of encrypted ballots and ballot IDs provided by the authenticator and the counter (who first decomposed, decrypted the ballots cast and tallies the results) with one another insuring that the lists are identical (i.e. no one tampered with the votes/ballots/election).

9. As per applicants arguments that the prior art of record does not teach the verifying that none of the ballots have been tampered with wherein the system reconstructs each ballot by (Pages 14-15; Claims 4, 18):

1. creating a new digital signature for the ballot (each ballot having a unique vote serial number/ballot ID) by signing the ballot using the server's public key; and

2. verifying the ballot's newly created digital signature against the originally cast ballot's digital signature using the server's private key.

Menezes et al. teach that the use of digital signatures as part of systems requiring information security is old and very well known in fact "Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation." (Menezes et al.: Page 425). Karro et al. utilizes the well-known public key encryption and digital signatures techniques to insure the integrity of the data received and/or to confirm/prove that the data was received as sent (Section 5.1 Data Protection, Page 6).

Menezes et al. that it is old and well know that the verification of a digital signature is purposed to ascertain if a given message has been signed by the private key that corresponds to a given public key and further that if one needs to verify whether some person has signed a given message, one only need obtain the person's public key. The verification of a digital signature is performed in (simplified) three steps (Menezes et al.: Pages 430-432):

1. calculate the current hash-value: a hash-value of the signed message is calculated. For this calculation, the same hashing algorithm is used as was used during the signing process.

2. calculate the original hash-value: the digital signature is decrypted with the same encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key used during the signing of the message. As a result, one obtains the original hash-value that was calculated from the original message during the first step of the signing process.

3. compare the current and the original hash-values: compare the current hash-value obtained in the first step with the original hash-value obtained in the second step. If the two values are identical, the verification if successful and proves that the message has been signed with the private key that corresponds to the public key used in the verification process. If the two values differ from one another, this means that the digital signature is invalid and the verification is unsuccessful.

10. As per applicants argument that the prior art of record does not disclose storing the individual's private encryption key, a certificate for the individual's public key and a voter identification generated when the voter registers for the system (Page 15) Karro et al. teaches that the system and method for securely voting over a network further comprises:

- the storage of the individual's private encryption key (floppy disk; Column 2, Page 4); and

- the registration of voters with the registrar prior to voting and that during the registration process qualified voters are assigned a "unique identification number" which along with the voter's name is placed in the registered voter's lists (Registration Phase Steps 1-2, Page 4), provided with a unique pair of public/private keys for the voter identification which are stored in a list (Registration Phase Steps 3-4, Page 4) and send to the voter for storage and use in the upcoming election(s).

Menezes et al. teach that the utilization of certificates in systems requiring information security is old and well-known and that "A public-key certificate consists of a data part and a signature part. The data part consists of the name of an entity, the public key corresponding to that entity, possibly additional relevant information (e.g., the entity's street or network address, a validity period for the public key, and various other attributes)." (Page 39) and that "Public-key certificates are a vehicle by which public keys may be stored, distributed or forwarded over unsecured media without danger of undetectable manipulation. The objective is to make one entity's public key available to others such that its authenticity (i.e. its status as the true public key of that entity) and validity are verifiable. In practice, X.509 certificates are commonly used (see page 587)." (Page 559; Figure 13.3 as shown below).

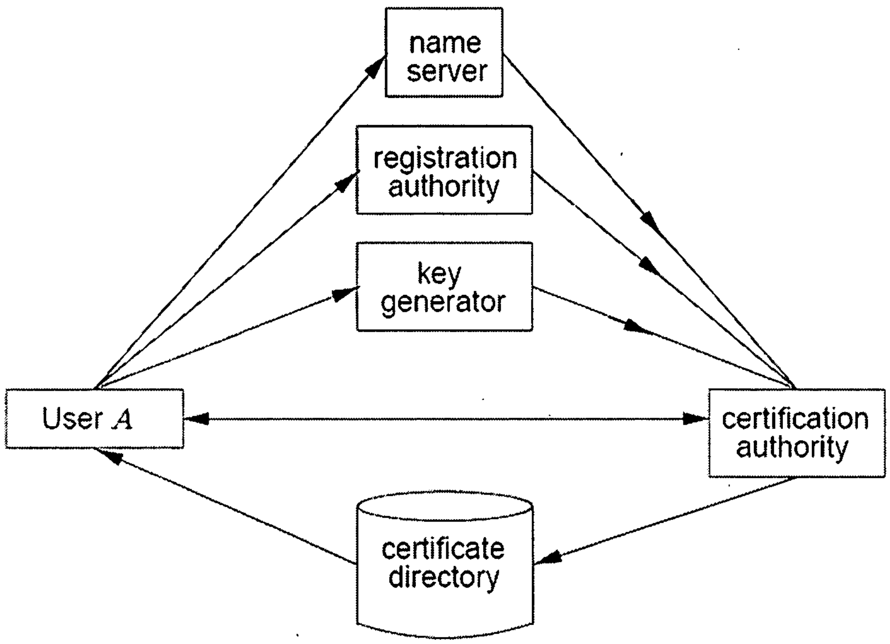

Figure 13.3: *Third party services related to public-key certification.*

Figure 3: Menezes et al.: Page 549

Shrader et al. teach a method and system for securely voting over a network wherein the system utilizes well-known public key encryption and digital signature techniques (Abstract). Shrader et al. further teach that the secure voting system utilizes digital certificates "To secure the integrity of the public key…A certificate (or public key certificate) is a data structure that is digitally signed by a certificate authority…" (Paragraph 0052).

11. As per applicants argument that the prior art of record does not teach the creation of a election voter table or comparing each ballot to the encrypted individual's voter identification to detect in an individual attempts to cast more than one ballot (Page

16) Karro et al. teach that the system and method for securely voting over a network utilizes a plurality of databases, databases implicitly having database tables for storing data) all of which are encrypted (Section 5.1 Data Protection, Page 6). More specifically Karro et al. teaches that one of the plurality of databases/data stores is a voter database (Figure 1, Voters DB, as shown below).

Karro et al. further teach that the system and method for securely voting over a network provides for a plurality of means for insuring the integrity and validity of the election including the authenticator subsystem's tracking/determining during the election for each voter if the voter has already voted ("If a voter tries to vote twice, the authenticator would notice the signature key s and ID have already been used.", Page 7, Lemma 2) and the registrars independent tracking of voters and their IDs that actually voted in the election.

12. As per applicant arguments that Sehr's definition of "demographics" is inconsistent with the use of demographics as recited in the specification, it is noted that the features upon which applicant relies (i.e. the optional inclusion of voter demographics that would not divulge the voter's identity) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). If the applicant feels the limitations to the voter demographic data are essential to the claimed invention it is suggested that the applicant amend the claims to include said limitation(s).

Further it is noted that if the limitations suggested by the specification where included in the claim(s) Karro et al. teaches the use of voter demographics as part of the registration process, the importance of the privacy of voter (demographic) information and the systems ability to insure the privacy of such information (System Requirements, Page 2; Section 5.1 Data Protection, Page 5; Lemma 4, Page 7).

13. As per applicants request for support of the officially noticed fact that the representation of documents as images (e.g. graphical ballots; Page 17) Karro et al. further teach a method and system for securely voting over a network is an improvement of (based upon) the Security-Conscious Election Polling System for the Internet (Sensus) system (protocol) developed and utilized by Cranor and Cytron (Karro et al.: Abstract). Cranor and Cytron, Sensus: Security-Conscious Election Polling System for the Internet (1997) teach that the Sensus protocol presents "...human readable ballots..." to voters wherein these human readable ballots can be displayed (represented, presented, etc.) in a plurality of ways including but not limited to text, multimedia (images, video, audio, text, etc.), HTML and the like (Cranor and Cytron: Paragraphs 1-2, Column 2, Page 4).

14. As per applicants request for support of the officially noticed fact that one-way hash functions are utilized, in systems requiring information security data, to insure data integrity.(Page 18) Menezes et al. teach that "One of the fundamental primitives in

modern cryptography is the cryptographic hash function, often informally called a one-way hash function." (Paragraph 1, Page 33).

Menezes et al. further teaches that "Hash functions are used for data integrity in conjunction with digital signature schemes, where for several reasons a message is typically hashed first, and then the hash-value, as a representative of the message, is signed in place of the original message (see Chapter 11). A distinct class of hash functions, called message authentication codes (MACs), allows message authentication by symmetric techniques. MAC algorithms may be viewed as hash functions, which take two functionally distinct inputs, a message and a secret key, and produce a fixed-size (say n-bit) output, with the design intent that it be infeasible in practice to produce the same output without knowledge of the key. MACs can be used to provide data integrity and symmetric data origin authentication, as well as identification in symmetric-key schemes (see Chapter 10)." (Pages 321-322).

More generally Menezes et al. teach that hash functions serve a plurality of functions in systems requiring information security including:

- "The most common cryptographic uses of hash functions are with digital signatures and for data integrity. With digital signatures, a long message is usually hashed (using a publicly available hash function) and only the hash-value is signed. The party receiving the message then hashes the received message, and verifies that the received signature is correct for this hash-value. This saves both time and space compared to signing the message directly, which would typically involve splitting the

message into appropriate-sized blocks and signing each block individually." (Page 33, Paragraph 4); and

- "A third application of hash functions is their use in protocols involving a priori commitments, including some digital signature schemes and identification protocols." (Page 33).

Menezes et al. further teaches "When used to detect whether the message input has been altered, they are called modification detection codes (MDCs). Related to these are hash functions which involve a secret key, and provide data origin authentication (x9.76) as well as data integrity; these are called message authentication codes (MACs)." (Page 33).

Claim Objections

15. Claim 14 is objected to because of the following informalities: claim 14 intended to claim "recording… the server's digital signature ~~signal~~ of the ballot…" Appropriate correction is required.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 1-6, 10-19 and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karro et al., Towards a Practical, Secure and Very Large Scale Online Election (1999).

Regarding Claims 1 and 15 Karro et al. teach the significant research, development and interest in electronic voting over computer networks (Introduction, Paragraph 3, Page 1). Karro et al. further teach the plurality of systems, methods and techniques for electronic voting systems (Introduction, Pages 1-2; Bibliography, Pages 8-9).

More specifically Karro et al. teach a system for securely voting over a network (online; Abstract, Page 1), comprising:

- six components/sub-systems: registrar, authenticator, matcher, distributor, verifier and counter (Section 4 The proposed protocol, Pages 4-5; Figures 1-3 Pages 4-5 and as shown below);

- delivering an electronic ballot from a server with a ballot identification number (vote serial number, ballot ID, b_ID; as shown in Figure 3 below; Pre-Voting Phase, Step 2, Page 4; Voting Phase Steps 1-4, Page 5);

- completing, digitally signing and submitting the ballot (Voting Phase Step 5, Page 5) and the ballot identification number; and

- creating of a plurality of data elements (records, stores, etc.) including but not limited to the ballot, voter ID, election choices, ballot ID, election ID, etc. (Voting Phase Step 5, Page 5; Section 5.1 Data Protection, Page 6; Figure 1, ID/Key DB, Page 4; Figures 1-3, Pages 4-5 and as shown below).

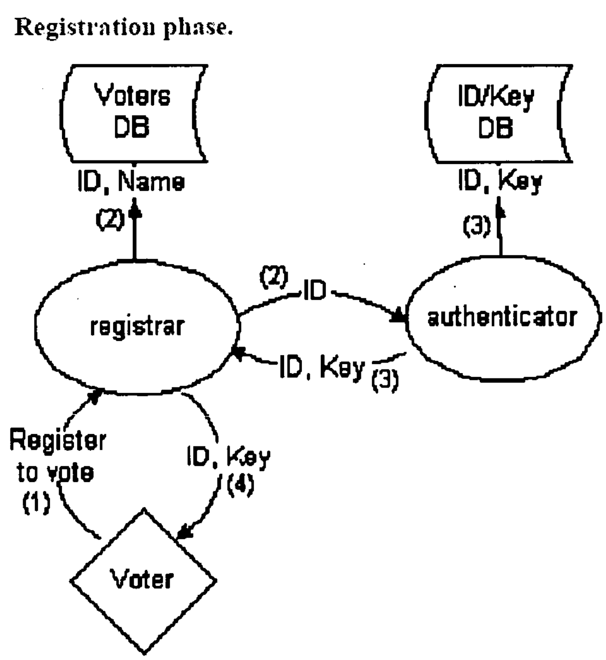

Figure 4: Registration Phase

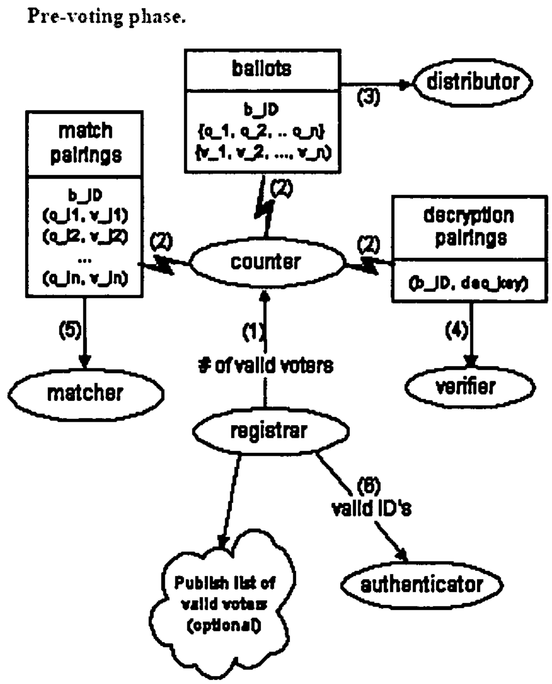

Figure 5: Pre-voting stage

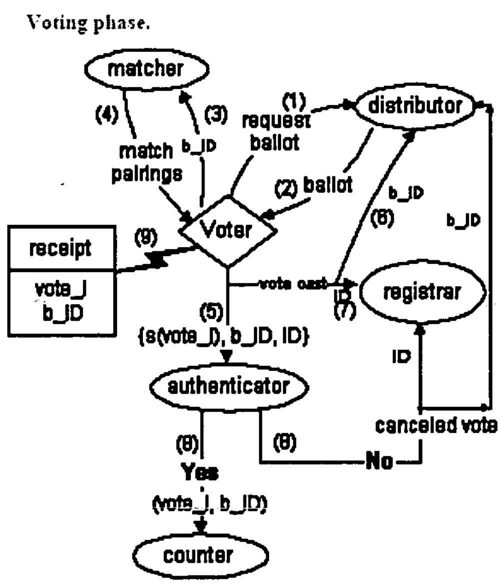

Figure 6: Voting Stage

Regarding Claims 2, 5, 16 and 19 Karro et al. teach the confirmation of the votes receipt and retention by the system to the voter. More specifically Karro et al. teaches communication with the voter if there is discovered to be an issue with the submitted vote as well as the transmission of a receipt confirming the vote's submission (Voting Phase, Steps 8-9, Page 5; Figure 3, Page 5 and as shown below).

Karro et al. further teach that the system for securely voting over a network further comprises:

- a minimum of two sub-systems the authenticator and the counter that publish the encrypted ballots and ballot ID numbers (Announcement Phase, Page 5);

- the voters ability to change his/her vote (Column 1, Page 8);

- the verification and confirmation of a vote by a voter (allowing the voter to decompose his/her vote; Announcement Phase, Page 5; Lemmas 3 and 5, Page 7); and

- the verification of the vote by the verification sub-system (Announcement Phase, Page).

Karro et al. teach a method and system for securely voting over a network (Abstract) wherein the system utilizes the well known and well established public key encryption scheme wherein voters are assigned a public/private pair key ("Eligible voters generate public/**private** key pairs for **signing** ballots...", Page 3, Paragraph 1; Registration Phase: Step 3 "the authenticator generates a unique pair of public/private keys for the ID it received (i.e. the voter's ID) and stores them....", Page 4; Registration Phase Step 4: "The registrar then send the pair (private/public key) to the voter....").

Regarding Claims 3-4 and 17-18 Karro et al. teach a variety of systems and methods for insuring the integrity and accuracy of an election. More specifically Karro et al. teach the use of the voter as discussed above as well as the authenticator, distributor, counter and verification sub-systems to insure the ballots have been cast, not tampered with and are accurately counted (Section 4 The proposed protocol, Pages 4-5; Lemmas 2, 3 and 5, Page 7; Column 2, Page 8; Figure 3, Page 5 and as shown above).

Karro et al. further teach the reconstruction of a ballot as a means for insuring the vote has not been tampered with as discussed above.

Regarding Claim 6 Karro et al. teach the storage of the voter's encryption key on a portable storage device and reading the device prior to voting (floppy disk; Column 2, Page 4).

Regarding Claim 10 Karro et al. teach that the accuracy of an election depends on its ability to process/handle three types of votes invalid (ineligible voters), votes made by eligible voters but in incorrect formats and votes generated for unused ballots (Lemma 3, page 7). Karro et al. further teach the detection of attempts to cast more than one ballot by the distributor, authenticator and registrar sub-systems (Voting Phase, Steps 6-7, Page 5; Announcement Phase, Page 5; Lemma 2, Page 7).

Karro et al. teach that the system and method for securely voting over a network utilizes a plurality of databases and subsequently database tables all of which are encrypted (Section 5.1 Data Protection, Page 6). More specifically Karro et al. teaches that one of the plurality of databases/data stores is a voter database (Figure 1, Voters DB, as shown below).

Karro et al. further teach that the system and method for securely voting over a network provides for a plurality of means for insuring the integrity and validity of the election including the authenticator subsystem's tracking/determining during the election for each voter if the voter has already voted ("If a voter tries to vote twice, the authenticator would notice the signature key s and ID have already been used.", Page 7, Lemma 2) and the registrars independent tracking of voter's and their IDs that actually voted in the election.

Regarding Claims 11 and 25 Karro et al. does not teach rendering the ballot as a bit map.

Official notice is taken that the representation (display, presentation, etc.) of a document as an image (i.e. graphical ballot) is old and well known in the art. One such use being the ability of graphical ballots to support a richer representation of the ballot through the use of multimedia ballots (e.g. multi-lingual support, pictures of candidates for illiterate voters, etc.).

It would have been obvious to one skilled in the art at the time of the invention that the system for secure voting over a network as taught by Karro et al. would have benefited from the use of a plurality of well known document representation techniques, technologies or methods including but not limited to the representation of a document as an image.

Further it would have been obvious to one skilled in the art at the time of the invention that the system for secure voting over a network as taught by Karro et al. would have benefited from the additional flexibility (e.g. multi-lingual ballots) that utilizing an image instead of plaintext for presenting and storing a ballot would have provided.

Regarding Claims 12 and 26 Karro et al. teach an online election system as discussed above. More specifically Karro et al. teach the presentation of ballots to voters utilizing Internet browsers (Netscape; Section 4 The proposed protocol, Page 4; Voting Phase, Page 5); the definition of an Internet browser being an application used for displaying HTML documents, and other WWW documents.

Regarding Claim 13, claim 13 recites similar limitations to Claims 1, 2 and 5 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1, 2 and 5.

Regarding Claim 14, claim 14 recites similar limitations to Claims 1, 3, and 4 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1, 3, and 4.

Regarding Claim 24 Karro et al. teach a plurality of means for insuring an individual does not cast more than one vote as discussed above.

Karro et al. does not teach the use of a one-way hash function as a means for identifying individuals who attempt to cast more than one vote.

Official notice is taken that one-way hash functions are widely used for data integrity in conjunction with digital signature schemes and that cryptographic hash functions generate a hash-value which serves as a compact representative image (sometimes called an imprint, digital fingerprint, or message digest) of an input string, and can be used as if it were uniquely identifiable with that string therefore providing a simple means for identifying identical records (attempts of individuals to cast more than one vote).

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from the additional security and accuracy provided by the use of one-way

hash functions as a means for identifying individuals who attempt to cast more than one vote (duplicate records).

Regarding Claim 27, claim 27 recites similar limitations to Claims 1, 2, and 5 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1, 2, and 5.

Regarding Claim 28, claim 28 recites similar limitations to Claims 1 and 4 and is therefore rejected using the same art and rationale as applied in the rejection of Claims 1 and 4.

18. Claim 7-8 and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karro et al., Towards a Practical, Secure and Very Large Scale Online Election (1999) as applied to claims 1-6, 10-19 and 24-28 above and further in view of London Shrader et al., U.S. Patent Publication No. 2002/007887.

Regarding Claims 7-8 and 20-21 Karro et al. teach an online system for securely voting over a network further comprising the storage pf the voter's encryption key on a portable storage device for access prior to voting as discussed above.

Karro et al. does not expressly teach the storage of additional information on a portable storage device, the use of a smart card or the use of certificates.

London Shrader et al. teach a system for secure voting over a network further comprising a plurality of user authentication and data encryption schemes including but not limited to:

- public/private key encryption systems and methods (Paragraph 0034, page 3; Paragraphs 0048-0050, Pages 4 and 5);

- digital certificates and certificate authorities (Paragraph 0017, Page 2; Paragraphs 0052---53, Page 5);

- Light-weight Directory Application Protocol (LDAP; Paragraphs 0052-0053, Page 5; Paragraph 0060, Page 5); and

- hash functions (Paragraph 0061, Pages 5-6).

London Shrader et al. further teach the utilization of smart cards as a means for storing and distributing digital certificates (Paragraph 0052, Page 5).

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from storage of additional information on a portable storage device, the use of a smart card and the use of digital certificates in view of the teachings of London Shrader et al. thereby improving the overall security of the system and making it possible for voters to securely vote from a plurality of locations.

Regarding Claim 22 Karro et al. does not teach the use of a certificate or that the certificate utilizes the Public-Key Infrastructure (X.509) standard.

Official notice is taken that the Public-Key Infrastructure (X.509) is old, very well known and widely used as a standard for defining digital certificates.

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from the use of a well known and accepted standard for creating and managing public-keys (X.509) thereby insuring the ability of the system to utilize the plurality of systems, tools and techniques based on the X.509 standard.

19. Claims 9 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Karro et al., Towards a Practical, Secure and Very Large Scale Online Election (1999), in view of London Shrader et al., U.S. Patent Publication No. 2002/007887 as applied to claims 1-8, 10-22 and 24-28 above, and further in view of Sehr, Richard Peter, U.S. Patent No. 5,875,432.

Regarding Claims 9 and 23 Karro et al. teach a system for securely voting over a network as discussed above.

Karro et al. does not teach the entering of demographic information onto the ballot.

Sehr teaches a secure voting system further comprising the collection of user demographic information (as shown below, Figure3; Figure 7, Element 204; Column 2, Lines 14-17; Claim 1) as a means for assisting in the verification of the identity of the voter (Column 6, Lines 3-14).

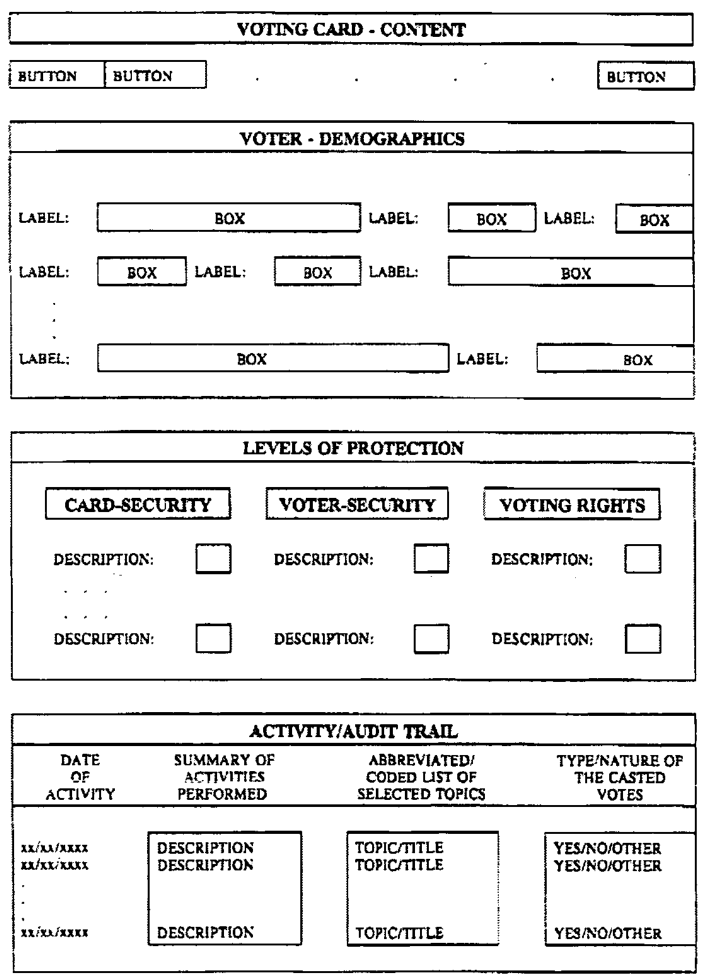

Figure 7: Voter Demographics

It would have been obvious to one skilled in the art at the time of the invention that the system for securely voting over a network as taught by Karro et al. would have benefited from the ability to utilize voter demographic information as an additional security measure thereby assisting in the verification of the identity of the voter in view of the teachings of Sehr.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott L. Jarrett whose telephone number is (571) 272-7033. The examiner can normally be reached on Monday-Friday, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (703) 305-9643. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SJ
4/18/2005

TARIQ R. HAFIZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600